IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
NEWNAN DIVISION

UNITED STATES OF AMERICA	:	
	:	
v.	:	Criminal Action No.
	:	3:21-CR-0004-TCB-RGV
ROBERT PURBECK	:	

SUPPLEMENTAL MOTION TO SUPPRESS SEARCHES OF COMPUTERS, PHONES, HARD-DRIVES, AND STORAGE DEVICES

In addition to the grounds he has previously raised in his motion to suppress the searches and seizures arising from the government's August 21, 2019 search of his home [Doc. 26], as amended [Doc. 38], Defendant Robert Purbeck hereby moves to suppress the results and fruits of the government's searches and data extractions of his computers, phones, hard-drives, and storage devices that occurred more than 14 days after the August 19, 2019 search warrant for his home was issued. In further support of this motion, Mr. Purbeck respectfully submits as follows.

Federal Rule of Criminal Procedure 41(e) requires that a search warrant be executed "within a specified time no longer than 14 days." Fed. R. Crim. P. 41(e). As the Eleventh Circuit recently held in United States v. Vedrine, No. 20-13259, 2022 WL 17259152 (11th Cir. Nov. 29, 2022), when discussing the extraction of data from a cellphone, "[l]aw enforcement complied with Rule 41(e) and

completed the data extraction within Rule 41(e)(2)(A)(i)'s 14-day timeline." Id. at *5. "Based on the plain language of the rule, we agree with our sister circuits that once the data is seized **and extracted** by law enforcement, the warrant is considered executed for purposes of Rule 41, and under Rule 41(e)(2)(B), law enforcement may analyze that data at a later date." Vedrine, supra, at *6 (emphasis added). Under Vedrine, the government must both seize and extract the contents of any electronic devices it seizes within 14 days of the issuance of the warrant, although it may wait and forensically analyze the extracted data at a later time. Id.

Mr. Purbeck's review of the discovery shows that, in almost all instances, law enforcement seized the physical computers, hard-drives, phones, and external storage devices on August 21, 2019, but did not extract any data from these devices within 14 days of the date the court issued the warrant, much less by August 30, 2019, the date that the judge issuing the warrant required for the warrant's execution. (See Exhibit F to Purbeck's December 13, 2021 Notice of Filing). The one exception to this appears to be the government's scanning of a Seagate Tower. However, even that data extraction apparently had to be done over because the government apparently deleted its initial extraction, thereby requiring another data extraction, which occurred more than 14 days following the issuance of the warrant and would therefore be illegal under Vedrine.

Specifically, it appears from the discovery produced by the government that, between August 27 and August 28, 2019, law enforcement extracted the data from the Seagate Tower (Gov't Evidence Item 1B198) that it seized on August 21, 2019 and placed that extracted data on hard drives labeled DEAT19, DEAT 21, and DEAT22. (See Exh. CC, attached hereto). So, that would be within the time required by the search warrant.

However, then it appears that law enforcement wiped that extracted information clean on or about September 17-18, 2019. (See Exh. DD, attached hereto, which are the first three pages of a 61-page document produced in discovery and refer specifically to DEAT19). Mr. Purbeck's interpretation of the wiping of the data extraction is corroborated by an FBI 302 created by FBI employee James Paul DeGrood on February 18, 2020, which reads in relevant part, as follows:

> A previous attempt was made to export the VMs on DEAT21 to DEAT22 on 10/3/19. Later it was seen that the disk appeared to be still in a wiped state. CS DeGrood exported the VMs found on DEAT21 to DEAT22 on 02/13/2020.

(See Exhibit EE, attached hereto).

As Mr. Purbeck understands these documents, although law enforcement imaged the Seagate Tower initially on August 27-28, 2019 (Exh. CC), it destroyed those images on September 17-18, 2019. (Exh. DD). It discovered that it had destroyed those images on or about October 3, 2019 and did not reimage the

Seagate Tower until February 13, 2020. (Exh. EE). If Mr. Purbeck is correct regarding the timing of the government's imaging of the Seagate Tower, then the government extracted the data from the Seagate Tower well after the time authorized by the original search warrant and without getting a new warrant. The untimely extraction of data from the Seagate Tower violates Federal Rule of Criminal Procedure 41(e), the Fourth Amendment, and the requirements set forth by the Eleventh Circuit in Vedrine, supra.

Similarly, the government has extracted data from other devices belonging to Mr. Purbeck well after the 14 days required by Rule 41(e), not to mention after the August 30, 2019 deadline set by the judge who issued the search warrant for Mr. Purbeck's residence. For example, on October 3, 2019, the government extracted the data from an "HP Laptop Elite Book" (Gov't Evidence Item 1B181) that they seized from Mr. Purbeck's residence on August 21, 2019. (See Exhibit FF, attached hereto). Also, on October 3, 2019, the government imaged the data from a "HP Z240 Tower S/N ZVA6060RF1" (Gov't Evidence Item 1B184) that they seized on August 21, 2019. (See Exhibit GG, attached hereto). Then, they imaged the data from that same HP Tower again on August 12, 2021. (See Exhibit HH). It is unclear whether they made the second image because they had destroyed the earlier image (ala the Seagate Tower), but regardless both extraction dates were

past the August 30, 2019 date authorized by the search warrant and also beyond the 14 days allowed by Rule 41(e). (See Exhs. GG and HH).

Additionally, on June 25, 2021, the government imaged a "Mac Book Pro S/N C02JKT67D853" (Gov't Evidence Item 1B185) that it seized from Mr. Purbeck's residence on August 21, 2019, almost two years earlier. (See Exhibit II, attached hereto). And on June 28, 2021 (almost two years after seizure), the government sought assistance from an FBI computer scientist to image a whole series of computers, hard-drives, and external storage devices. (See Exhibit JJ, attached hereto). All of these searches were well outside of the legal time for extracting the data from these devices using the authority granted by the August 19, 2021 search warrant issued by the federal court in Idaho. Mr. Purbeck is not aware of any new search warrant that would authorize these searches. Accordingly, under the authority of Vedrine, the government's belated imaging and data extractions from Mr. Purbeck's computers and storage devices violates both Federal Rule of Criminal Procedure 41 and the Fourth Amendment.

The Eleventh Circuit's recent decision in Vedrine is of particular significance here because it conflicts with this Court's older decision in United States v. Dixon, No.: 3:20-cr-3-TCB, 2021WL1976679 (N.D. Ga. May 18, 2021). In Dixon, this Court held that the government's two-year delay in searching the defendant's I-phone was not unreasonable given that it was password protected and

the defendant had not provided the government with the password. Dixon, supra, at *2. In contrast to Dixon, Mr. Purbeck had provided his passwords to the government. Even more importantly, however, subsequent to Dixon, the Eleventh Circuit decided Vedrine, in which the Circuit Court stated, "[b]ased on the plain language of the rule, we agree with our sister circuits that once the data is seized **and extracted** by law enforcement, the warrant is considered executed for purposes of Rule 41, and under Rule 41(e)(2)(B), law enforcement may analyze that data at a later date. Vedrine, supra, at *6 (emphasis added).

As best as Mr. Purbeck can tell, the government did not seize and extract the contents of any of the devices it seized from Mr. Purbeck on August 21, 2019 within the 14 days of the date the search warrant was issued (September 2, 2019), much less by August 30, 2019 – the time set by the judge who issued the search warrant for Mr. Purbeck's home. For the one device that they did extract data from prior to August 30, 2019 (the Seagate Tower), it appears they destroyed that extracted data and re-extracted the data from the Seagate Tower on a date more than 14 days after the search warrant was issued and without obtaining a new warrant authorizing the re-extraction, thereby rendering the later extraction illegal.

Mr. Purbeck's position is that, under Vedrine, the government's extraction of data more than 14 days following the issuance of the search warrant is unreasonable, violates Rule 41, violates the terms of the search warrant, and

violates the Fourth Amendment. Accordingly, the Court should suppress all data extractions that occurred after September 2, 2019, which was the fourteenth day following the search warrant being issued on August 19, 2019.

Additionally, not only has the government not extracted the data from Mr. Purbeck's various devices within 14 days of the date the search warrant was issued, as it was required to do by Rule 41 and Vedrine, the government also appears, for the most part, not to have timely analyzed or examined the data that it did extract. Although both Rule 41 and Vedrine allow law enforcement to examine/forensically analyze the extracted data at a later time, that later examination must still occur within a reasonable period of time. Not forensically analyzing the extracted data within a reasonable time violates the Fourth Amendment and provides yet another basis to suppress the searches of both phones and the information gleaned therefrom. See Vedrine, supra, at *5-6 (the Eleventh Circuit specifically noting that, assuming arguendo that any seized data must be reviewed in a reasonable period of time, the "review of data within a matter of weeks" is "clearly different" from a 15-month delay that the district court found unreasonable in United States v. Metter, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012)). Here, although Mr. Purbeck has been unable to determine exactly how much time has gone by before the government forensically analyzed the data it extracted, with the exception of the data the government forensically examined in March, 2020, it appears that the

delay is more than a matter of weeks (see Vedrine, supra, at *5-6, finding delay not unreasonable), and it also appears to be closer to 15 months or more (see Metter, 860 F. Supp. 2d at 212-216, finding delay unreasonable). Accordingly, Mr. Purbeck moves to suppress the forensic examinations of any data extracted from his devices because (in addition to the delay in extracting the data), the delay in examining/analyzing that data was unconstitutionally unreasonable and violated the Fourth Amendment. At a minimum, an evidentiary hearing is required to determine whether the government has analyzed the data that it untimely extracted within a reasonable time and, if not, why not.

Mr. Purbeck has sought the return of his property, including but not limited to his computers, hard-drives, phones, and storage devices. No later than January 31, 2021, Mr. Purbeck had filed a motion pursuant to Federal Rule of Criminal Procedure 41 seeking the return of his property. (See Doc. 2 in 1:21-CV-0047-BLW (District of Idaho)). Also, to the extent the government may contend, as it apparently has in response to his civil filings, that his interest in his property has been diminished by virtue of his property being listed as subject to forfeiture in the indictment in this case, Mr. Purbeck respectfully submits that the government cannot know whether something is subject to forfeiture when it has not even searched it before claiming it is forfeitable. Accordingly, his interest in his property is undiminished.

As the Eleventh Circuit noted long before Vedrine, "[c]omputers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives. Thus, the detention of the hard drive for over three weeks before a warrant was sought constitutes a significant interference with [the defendant's] possessory interest." United States v. Mitchell, 565 F.3d 1347, 1350–51 (11th Cir. 2009). Here, the government failed to extract the contents of many of Mr. Purbeck's computers and other devices (storage and otherwise) in a timely fashion, and they failed to examine the contents of these devices in a timely fashion.

Mr. Purbeck requests that the Court hold an evidentiary hearing on this motion and thereafter grant this motion and suppress all evidence arising from these searches.

WHEREFORE, Mr. Purbeck respectfully requests that the Court (1) hold an evidentiary hearing on all matters raised in his motion to suppress and any others that may be developed at the hearing, (2) establish a briefing schedule for all parties to address the issues raised in this motion to suppress and developed at the evidentiary hearing, and (3) thereafter grant this motion and suppress and exclude

from evidence any and all information, material, items, or evidence gathered from the illegal detentions, searches, seizures and interrogations detailed in this motion.

Respectfully submitted, this 26th day of July, 2023.

/s/ *Andrew C. Hall*
Andrew C. Hall
Georgia Bar No. 318025
Hall Hirsh Hughes, LLC
150 E. Ponce de Leon Ave., Suite 450
Decatur, Georgia 30030
404/638-5880 (tel.)
404/638-5879 (fax)
andrew@h3-law.com
Counsel for Defendant Robert Purbeck

CERTIFICATE OF COMPLIANCE WITH TYPE AND FONT

AND CERTIFICATE OF SERVICE

I hereby certify that this motion has been prepared in Times New Roman font (14 pt.) and consistent with the Local Rules of this Court.

I further hereby certify that I have this date caused a true and correct copy of the foregoing SUPPLEMENTAL MOTION TO SUPPRESS SEARCHES OF COMPUTERS, PHONES, HARD-DRIVES, AND STORAGE DEVICES to be served by filing it with the Clerk of Court and emailing separately to:

Assistant United States Attorney Michael Herskowitz and Alex Sistla

This 26th day of July, 2023.

/s/ Andrew C. Hall
Andrew C. Hall